THE NATIONAL LAW JOURNAL

NOVEMBER 24, 2014

An ALM Publication

CYBER SECURITY

A SPECIAL REPORT

Target. Michaels Stores. Neimann-Marcus. Home Depot. Data breaches at these and other retailers compromised millions of consumers within the past 12 months, and caused billions of dollars in losses. In this special section, legal specialists discuss some of the dangers facing corporations and their attorneys, and offer advice on how to mitigate this potentially disastrous legal risk.

ISTOCKPHOTO/HLIB SHABASHNYI

Boards of Directors Can't Shirk Cyber Responsibility

BY REECE HIRSCH

There was a time, not so long ago, when cybersecurity was an arcane topic that was primarily the province of a company's information-technology department. Those days are gone. Cybersecurity is now a board-level concern, given the litany of headline-grabbing cybersecurity breaches, the skyrocketing costs of cybercrime and the far-reaching repercussions of a severe or poorly handled cybersecurity breach.

Corporate boards have a duty to protect corporate assets and, increasingly, those assets take the form of information. Ever more companies are data-driven, with business models built upon the collection and use of personal information. Even for companies outside the technology sector, computers and software are integral to operations and mission-critical functions are computerized. Most companies also have sensitive electronic data they must protect, from trade secrets to employees' personal information.

Several recent security breaches have been followed by shareholder derivative lawsuits against corporate directors and officers, alleging that failure of oversight and inadequate cybersecurity systems led to breaches. Proxy advisory services have also questioned board conduct following certain security breaches. Although most of the derivative lawsuits have either settled or have not progressed far beyond the pleading stages, boards should not wait for case law to define their responsibilities with respect to cybersecurity, given the ever-growing nature of the threat and related costs.

ZACHARY D. PORTER / DAILY REPORT

U.S. Securities and Exchange Commissioner Luis Aguilar

According to a 2012 survey by the Ponemon Institute, U.S. companies experienced a 42 percent increase between 2011 and 2012 in the number of successful cyberattacks they experienced per week. The average annualized cost of cybercrime to a sample of U.S. companies was $11.6 million per year, representing a 78 percent increase since 2009, according to a 2013 survey by Hewlett-Packard Co. The Center for Strategic International Studies estimated that cybercrime costs the global economy as much as $575 billion annually and approximately $100 billion in the United States alone.

In a June 2014 speech at the New York Stock Exchange on "Cyber Risks and the Boardroom," U.S. Securities and Exchange Commissioner Luis Aguilar summed up the imperative facing directors: "Given the significant cyberattacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyberattacks, ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk-oversight responsibilities."

So what can a board of directors do to address the emerging risk area of cybersecurity?

Remove the intimidation factor. In a recent

panel discussion of the National Association of Corporate Directors, several factors were cited as contributing to a general reluctance among directors to address cybersecurity. First, cybersecurity experts often use technical jargon that can be difficult for the nontech-savvy to understand. Second, directors, particularly those in mature companies, tend to be older and not as comfortable with technology. Third, information technology is constantly evolving and few directors who are not also I.T. professionals can devote the time necessary to remain thoroughly conversant in the area.

It's important to remember that directors are not required to become cybersecurity experts and are entitled to rely on management and outside experts for advice. Given the growing significance of cybersecurity risks, the board should develop a high-level understanding of those risks through briefings from management and others. Boards should have adequate access to expertise and discussions about cyberrisk management should be given regular and adequate time on the board agenda.

OUTSIDE CONSULTANTS

Consider external evaluation of security risk management. Outside consultants are available to audit a company's cybersecurity practices and should be considered. Even if a board chooses not to engage a consultant, directors should be careful about relying too heavily for education and assessment upon the company's I.T. and security employees whose work is being evaluated. Overreliance on internal security personnel can sometimes even lead to overspending on security when an in-house security professional interprets legal standards and organizational risks as an opportunity to secure funding for a "wish list" of cybersecurity measures.

Develop a stress-tested incident response plan. Aguilar noted that the primary distinction between a cyberattack and other crises a company may face is the speed with which the company must respond, to contain the rapid spread of damage. Companies must be prepared to respond within hours, if not minutes, to a cyberevent — to detect it, analyze it, halt further damage and prepare a response. That means that an organization must have an incident-response plan that has been thoughtfully developed, tested in advance and ready for deployment when the inevitable security breach occurs. The incident-response team should include representatives of the various units of a company affected by a significant breach, including legal, compliance, I.T. and security, human resources, media relations and (for public companies) investor relations.

The incident-response team should meet regularly in "peacetime" in advance of a cybersecurity breach so that everyone understands their roles and is prepared to respond quickly.

Use the NIST cybersecurity framework as a road map. In February 2014, the National Institute for Standards and Technology (NIST) released the Framework for Improving Critical Infrastructure Cybersecurity. The framework is intended to provide companies with a set of industry standards and best practices for managing cybersecurity risks. Although the NIST framework is voluntary and primarily directed to companies such as utilities that are part of the nation's critical infrastructure, some commentators have already suggested that it will become a baseline for corporate best practices and may be used in assessing legal and regulatory exposure, and insurance coverage, with respect to cyber liability. As Aguilar noted, at a minimum, a board should work with management to assess how corporate policies match the framework's guidelines and whether additional work may be needed.

Model the risk scenarios relevant to your company. Every company has a different cybersecurity risk profile depending upon the information it maintains and the manner in which it which uses and maintains those data. Directors should work with managers to model the scope and liability risk to the company arising from a significant cybersecurity breach before they actually face such an event in real time. Once the risks have been quantified, consider what risks can be avoided, accepted, mitigated or transferred through insurance. A board should consider and regularly reevaluate the appropriateness of cyber liability insurance.

SET THE TONE FROM THE TOP

Address cybersecurity as an enterprise-wide management issue, not an I.T. issue. Although many aspects of cybersecurity are technical systems issues that may be best addressed by I.T. and security professionals, cybersecurity is also an enterprisewide business and risk-management issue that "starts at the keyboard" with the company's employees. Boards can help create a cybersecurity culture within an organization by ensuring that workforce members are given regular security training. In light of the need for fast response to a cybersecurity breach, it is particularly critical that employees be trained to recognize one when they encounter it and report the incident to the appropriate member of the company's incident response team.

Structure your board and committees to address cybersecurity. The board of directors' risk-oversight function often either lies with the full board or is delegated to the audit committee. Unfortunately, both the board and audit committee may lack the technical expertise or resources to adequately manage cybersecurity risk. Such deficiencies may be addressed by conducting cybersecurity education for the board or by recruiting board members specifically based upon their knowledge of cybersecurity.

Another approach cited by Aguilar is the creation of a separate enterprise risk committee on the board that would develop a "big picture" approach to cybersecurity and other companywide risks. One study by Deloitte indicates that 48 percent of corporations have board-level risk committees responsible for privacy and security risks, up from a mere 8 percent that reported having such a committee in 2008.

The importance of properly structuring board risk oversight functions was highlighted in 2009, when the Securities and Exchange Commission amended its rules to require public companies to disclose information about the board's role in risk oversight, including a description of whether and how the board administers its oversight function, such as through the whole board, a separate risk committee or the audit committee. It should be remembered that, while cybersecurity is technical, rapidly evolving and increasingly critical, it ultimately is just another liability risk that boards must manage. Boards that address cybersecurity with due diligence and care should be confident that their decisions will enjoy the traditional protections of the business-judgment rule.

However, as Aguilar put it, "Boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility do so at their own peril."

Reece Hirsch is a partner in the San Francisco office of Morgan, Lewis & Bockius and co-leader of the privacy and cybersecurity practice. He advises companies on a wide range of privacy and cybersecurity issues and has served on advisory groups to the California Office of Privacy Protection that developed breach-response recommended practices.